CLAIMS

1. A method of generating a secure transaction log recording transaction data established between a first (10) and a second (20) data processing device, comprising the steps of:

the first device issuing a partial transaction log (63) to the second device, the partial transaction log including identification data and event data associated with the transaction;

the second device issuing to the first device, in response to the partial transaction log, a signed full log (66), the signed full log including said identification data and event data, secured by a first digital signature specific to the second device (20); and

the first device issuing, in response to the signed full log (66), a re-signed full log (67) including said identification data, said event data and said first digital signature, secured by a second digital signature specific to the first device.

2. The method of claim 1 further including, prior to the step of issuing the partial transaction log (63), the step of:

establishing communication (61,62) between the first and second devices in order to effect a transaction and generate data associated with that transaction, at least some of the data so generated being used as said event data in said partial transaction log.

3. The method of claim 2 in which the transaction includes authentication (62) of the identity of at least one of the devices.

4. The method of claim 1 in which the event data includes time stamp information derived from at least one of the first device (10) and the second device (20).

5. The method of claim 1 in which the event data and/or the further event data includes time stamp information derived from both the first device (10) and the second device (20).

6. The method of claim 1 in which the identification data includes data uniquely identifying the first device (10) and/or the second device (20).

7. The method of claim 1 in which the signed full log includes further event data added by the second device (20).

8. The method of claim 1 in which at least one or more of: the partial log; the signed transaction log; and the re-signed transaction log are encrypted during transfer between the first (10) and second (20) devices.

9. The method of claim 1 in which the first digital signature is applied using a private key of the second device, the counterpart public key being accessible to the first device.

10. The method of claim 1 or claim 9 in which the second digital signature is applied using a private key of the first device, the counterpart public key being accessible to the second device.

11. The method of claim 1 further including the steps of:

issuing a data request (64) to a third device (40), by the second device (20), after receiving the partial transaction log (63) from the first device;

receiving (65) third party event data, by the second device from the third device (40) in response to the data request;

including the third party event data into the signed full log (66) issued to the first device.

12. The method of claim 11 in which the third party event data is secured by a third digital signature specific to the third device (40).

13. The method of claim 11 in which the third party event data includes time stamp information independent of the first and second devices.

14. The method of claim 11 in which the third party event data includes transaction authorisation data.

15. The method of claim 12 in which the third digital signature is applied using a private key of the third device (40), the counterpart public key being accessible to the first (10) and second (20) devices.

16. The method of claim 1 in which the first device (10) is a portable identification device and the second device (20) is an access control device for controlling access to a building, facility or resource.

17. The method of claim 1 or claim 11 in which the signed full log includes the contents of the partial transaction log modified by the second device.

18. The method of claim 1 or claim 11 further including the steps of:

the first device (10) issuing a revised transaction log to the second device, after receiving the signed full log (66), the revised partial log comprising the contents of the signed full log modified by the first device; and

the second device (20) issuing to the first device, in response to the revised partial log a revised signed full log secured by a digital signature specific to the second device.

19. The method of claim 18 further including repeating the steps of issuing a revised partial transaction log and a revised signed full log until both the first and second devices are in agreement with the contents of the transaction log.

20. A method of operating an access control device (20) to generate a secure transaction log recording transaction data established between a first device (10) and the access control device (20), comprising the steps of:

receiving from the first device, a partial transaction log (63), the partial transaction log including identification data and event data associated with the transaction;

issuing to the first device, in response to the partial transaction log, a signed full log (66), the signed full log including said identification data and event data, secured by a first digital signature specific to the access control device; and

receiving, from the first device, in response to the signed full log, a re-signed full log (67) including said identification data, said event data and said first digital signature, secured by a second digital signature specific to the first device.

21. The method of claim 20 further including the steps of:

issuing a data request (64) to a third device, after receiving the partial transaction log (63) from the first device;

receiving third party event data (65), from the third device in response to the data request;

including the third party event data into the signed full log (66) issued to the first device.

22. The method of claim 20 or claim 21 in which the signed full log includes the contents of the partial transaction log modified by the second device (20).

23. The method of claim 20 or claim 21 further including the steps of:

the first device (10) issuing a revised partial transaction log to the second device, after receiving the signed full log (66), the revised partial log comprising the contents of the signed full log modified by the first device; and

the second device (20) issuing to the first device, in response to the revised partial log a revised signed full log secured by a digital signature specific to the second device.

24. The method of claim 23 further including repeating the steps of issuing a revised partial transaction log and a revised signed full log until both the first (10) and second (20) devices are in agreement with the contents of the transaction log.

25. The method of claim 20 further including the step of verifying the authenticity and integrity of the re-signed full log using a public key of the first device.

26. The method of claim 20 or claim 21 in which the access control device (20) is any of an electronic door lock, electronic gate lock, equipment control system, computer system, data processing or retrieval system, point of sale terminal, or vending machine, and in which the first device (10) is any of an electronic key, credit or debit card.

27. The method of claim 20 further including the step of allowing the first device (10) access to a predetermined resource, by the access control device (20), only after receipt of the re-signed log by the access control device.

28. A method of operating a first data processing device to generate a secure transaction log recording transaction data established between the first device (10) and a second data processing device (20), comprising the steps of:

issuing a partial transaction log (63) to the second device, the partial transaction log including identification data and event data associated with the transaction;

receiving from the second device, in response to the partial transaction log, a signed full log (66), the signed full log including said identification data

and event data, secured by a first digital signature specific to the second device; and

issuing, in response to the signed full log, a re-signed full log (67) including said identification data, said event data and said first digital signature, secured by a second digital signature specific to the first device.

29. The method of claim 28 further including the step of verifying the authenticity and integrity of the signed full log using a public key of the second device.

30. A computer program product, comprising a computer readable medium having thereon computer program code means adapted, when said program is loaded onto a computer, to make the computer execute the procedure of any one of claims 20 to 29.

31. Apparatus for generating a secure transaction log recording transaction data established between a first (10) and a second (20) data processing device, comprising:

means (11), in the first device, for issuing a partial transaction log to the second device, the partial transaction log including identification data and event data associated with the transaction;

means (21), in the second device, for issuing to the first device, in response to the partial transaction log, a signed full log, the signed full log including said identification data and event data, secured by a first digital signature specific to the second device; and

means (11), in the first device, for issuing, in response to the signed full log, a re-signed full log including said identification data, said event data and said first digital signature, secured by a second digital signature specific to the first device.

32. An access control device (20) adapted to generate a secure transaction log recording transaction data established between a first device (10) and the access control device, comprising:

means (21,25) for receiving from the first device, a partial transaction log, the partial transaction log including identification data and event data associated with the transaction;

means (21) for issuing to the first device, in response to the partial transaction log, a signed full log, the signed full log including said identification data and event data, secured by a first digital signature specific to the access control device; and

means (21) for receiving, from the first device, in response to the signed full log, a re-signed full log including said identification data, said event data and said first digital signature, secured by a second digital signature specific to the first device.

33. A data processing device (10) adapted to generate a secure transaction log recording transaction data established between the data processing device and a second data processing device (20), comprising:

means (11,15) for issuing a partial transaction log to the second device, the partial transaction log including identification data and event data associated with the transaction;

means (11) for receiving from the second device, in response to the partial transaction log, a signed full log, the signed full log including said identification data and event data, secured by a first digital signature specific to the second device; and

means (11) for issuing, in response to the signed full log, a re-signed full log including said identification data, said event data and said first digital signature, secured by a second digital signature specific to the data processing device.